Notice of Allowability	Application No.	Applicant(s)	
	09/895,801	BROWN ET AL.	
	Examiner	Art Unit	
	Ali S. Abyaneh	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *10-02-2006*.

2. ☒ The allowed claim(s) is/are *13,15-20,30,31 and 34*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☒ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☒ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

EXAMINER'S AMENDMENT

1. The application has been amended as follows:

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with applicant's attorney Gregory T. Fettig on 05-30-2007 and 05-31-2007.

Claim 13 is amended to:

A method for use in a multi-level secure system for sanitizing a message, ~~said multi-level secure system including at least first and second security levels wherein first security level users are authorized to receive sensitive information that second security level users are not authorized to receive,~~ said method comprising the steps of:

establishing a computer-based sanitization tool for sanitizing messages based on predefined sanitization rules, wherein said multi-level secure system includes at least first and second security levels and wherein first security level users are authorized to receive sensitive information that second security level users are not authorized to receive;

first using said computer-based sanitization tool for receiving a message for potential distribution;

second operating said computer-based sanitization tool for identifying at least first and second potential recipients having first and second security clearances, respectively;

third operating said computer-based sanitization tool for sanitizing said received message to generate a first sanitized message for

transmission to said first potential recipient; and

fourth operating said computer-based sanitization tool for sanitizing said received message to generate a second sanitized message, different than the first sanitized message, for transmission to said second potential recipient,

wherein said step of third operating comprises identifying first sensitive information within said message based on said first security clearance of said first potential recipient and protecting said first sensitive information such that said first sensitive information is not useable by said first potential recipient, and said step of fourth operating comprises identifying second sensitive information based on said second security clearance of said second potential recipient and protecting said second sensitive information such that said second sensitive information is not useable by said second potential recipient.

Claim 30 is amended to:

A method for use in a multi-level secure system for sanitizing a message, said method comprising steps of:

receiving an input file that includes information associated with at least first and second security levels of the multi-level secure system, wherein a user associated with said first security level of the multi-level secure system is entitled to receive information that a user associated with said second security level of the multi-level secure system is not entitled to receive;

determining a security level associated with at least one user of the multi-level secure system to be said first security level;

determining a security level associated with at least one user of the multi-level secure system to be said second security level;

generating a first output file from the input file based on the first

security level;

transferring the first output file to said at least one user with the first security level;

parsing intelligible elements from the information of the input file;

analyzing said intelligible elements to select a portion of the intelligible elements for sanitization according to the second security level;

sanitizing the information of the selected portion of the intelligible elements according to the second security level to generate a second output file for said at least one user ~~of the multi-level secure system~~ with the second security level, wherein said second output file has a first format; and

formatting the second output file to a second format for said at least one user ~~of the multi- level secure system~~ with the second security level; and

transferring the second output file in the second format to said at least one user with the second security level ~~of the multi level secure system~~.

Claim 31 is amended to:

A method for use in a multi-level secure system for sanitizing a message, said method comprising the steps of:

establishing rules based logic ~~for use in~~ determining a level of access to sensitive information as a function of information regarding an intended recipient of a message including at least a portion of said sensitive information, wherein different recipients are associated with different levels of access to said sensitive information, said rules based logic ~~further being operative for~~ analyzing specific items of said sensitive

information in the context of a given message relative to a selected rule set of a number of rule sets, wherein different ones of said rule sets correspond to set different levels of access to said sensitive information;

receiving, in a processing system including said rules based logic, a first message including a first item of said sensitive information;

analyzing, in said processing system, said first message to obtain recipient information regarding a first intended recipient of said first message;

based on said recipient information, accessing a first rule of a first rule set of said number of rule sets using said processing system;

applying said first rule to process said first item of sensitive information, using said processing system, so as to generate a processed first message having a difference in relation to said first message, said difference being a function of said recipient information regarding said first intended recipient; ~~and~~

processing the said first item of sensitive information according to the first rule, wherein said processing includes altering the first item of sensitive information or removing the first item of sensitive information;

processing the first message according to a second rule associated with a second recipient to generate a second message that differs from the first message; and

operating said processing system to cause said processed first message to be transmitted to said first intended recipient.

Claim 34 is amended to:

A method as set forth in Claim ~~33~~ 31, wherein processing the first message includes processing a second item of sensitive information according to the second rule, wherein said processing the second item of sensitive information includes altering the second item of sensitive information or removing the second item of sensitive information.

Claims 14, 32 and 33 are cancelled.

Examiner comment in regard to the drawing

2. Drawing presented in this application is informal therefore a new corrected drawing in compliance with 37 CFR 1.121(d) is required in this application.

Allowable Subject Matter

3. Claims 13, 15-20, 30, 31 and 34 are allowed.

The following is an examiner's statement of reasons for allowance:

The prior art Fahlman et al. (US Patent NO 5,960,080) of record discloses, a method and an apparatus for transforming an original message to a final message by separating sensitive information from the message prior to an untrusted service, so that the confidentiality of the information is maintained. Transforming an original message to a final message includes the steps of

identifying sensitive terms in original message, replacing sensitive terms with a token to create sanitized message; storing sensitive terms; transmitting the sanitized message to a provider of the untrusted service; performing untrusted services on the sanitized message to create service message; merging the serviced message with the sensitive terms stored to create final message.

The prior art Thuraisngham et al. (US Patent NO 5,355,474) of record discloses, an apparatus for an integrated architecture for an extended multilevel secure database management system. The multilevel secure database management system processes security constraints to control certain unauthorized inferences through logical deduction upon queries by users and is implemented when the database is queried through the database management system, when the database is updated through the database management system, and when the database is designed using a database design tool.

However, prior arts taken singly or in combination, fail to anticipate or render the following limitation:

As per claim 13,

sanitization tool for identifying at least first and second potential recipients having first and second security clearances, respectively; identifying first sensitive information within the said message based on said first security clearance of said first potential recipient and protecting said first sensitive

information such that said first sensitive information is not useable by said first potential recipient, and said step of fourth operating comprises identifying second sensitive information based on said second security clearance of said second potential recipient and protecting said second sensitive information such that said second sensitive information is not useable by said second potential recipient.

As per claim 30,

receiving an input file that includes information associated with at least first and second security levels of the multi-level secure system; determining security level associated with at least one user of the multi-level secure system to be said first security level; determining a secure level associated with at least one user of the multi-level secure system to be said second security level, generating a first output file from the input file based on the first security level and generate a second output file for said at least one user with the second security level, wherein said second output file has a first format; and formatting the second output file to a second format for said at least one user with the second security level.

As per claim 31,

analyzing, in said processing system, said first message to obtain recipient information regarding a first intended recipient of said first massage; based on the said recipient information, accessing a first rule set of said number of rule set using said processing system; applying first rule to process said first

item of sensitive information; processing the said first item of sensitive information according to the first rule,; processing the first message according to a second rule associated with a second recipient to generate a second message that differs form the first message.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 2727961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865.3he fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about

the PAIR system, see hftp://pair-direct.uspto.gbv. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AA

Ali Abyaneh
Patent Examiner
Art Unit 2137
06/04/07

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER